Agence de cybersécurité de l'UE (ENISA) et certification de cybersécurité des TIC ("Cybersecurity Act")

2017/0225(COD) - 13/09/2017 - Document de base législatif

OBJECTIF: réformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en vue de doter l'UE d'une capacité accrue en matière de cybersécurité et définir un cadre pour la mise en place d'un système européen de certification en matière cybersécurité.

ACTE PROPOSÉ: Règlement du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN: le Parlement européen décide conformément à la procédure législative ordinaire et sur un pied d'égalité avec le Conseil.

CONTEXTE: l'Union européenne a déjà pris un certain nombre de mesures pour accroître la résilience face aux cyberattaques. Depuis la première stratégie européenne de cybersécurité adoptée en 2013, des développements importants ont eu lieu, y compris le deuxième mandat de l'Agence européenne pour la sécurité des réseaux et de l'information (**ENISA**) et l'adoption de la directive sur la sécurité des réseaux et des systèmes d'information (Directive SRI) qui constituent la base de la présente proposition.

En 2016, la Commission européenne a adopté une communication **sur le renforcement du système européen de cyber-résilience**, dans laquelle d'autres mesures ont été annoncées pour mieux protéger l'UE.

Le Conseil a rappelé que le règlement (UE) n° 526/2013 sur l'ENISA était l'un des éléments essentiels d'un cadre de résilience informatique de l'UE et a demandé à la Commission de prendre d'autres mesures pour aborder la question de la certification au niveau européen. En 2017, il s'est félicité de l'intention de la Commission d'examiner la stratégie de la cybersécurité en septembre et de proposer d'autres actions ciblées avant la fin de 2017.

ANALYSE D'IMPACT: l'analyse d'impact a identifié plusieurs problèmes tels que: la fragmentation des politiques et des approches de la cybersécurité dans les États membres; des ressources dispersées et des approches disparates au sein des institutions, organismes et organes de l'UE; une sensibilisation et une information insuffisantes des citoyens et des entreprises, conjuguée à l'émergence croissante de multiples systèmes nationaux et sectoriels de certification.

L'analyse a permis de conclure qu'une **ENISA réformée combinée à un cadre général de certification de la cybersécurité de l'UE** en matière de technologies de l'information des communications (TIC) était l'option privilégiée.

CONTENU: la proposition vise à **réviser le mandat actuel de l'ENISA** et à définir un ensemble renouvelé de tâches et de fonctions, en vue de soutenir efficacement les États membres, les institutions de l'UE et les efforts des autres parties prenantes dans l'objectif d'assurer un cyberespace sécurisé dans l'Union européenne.

Le nouveau mandat proposé vise à donner à l'Agence **un rôle plus important et plus central**, notamment en contribuant à la mise en œuvre de la directive SRI, et en devenant un centre d'expertise pour aider les États membres et la Commission à créer et à appliquer le cadre de certification à l'échelle de l'UE.

En particulier, la proposition vise à:

- **transformer l'actuelle Agence européenne pour la sécurité des réseaux et de l'information (ENISA) en une Agence européenne de la cybersécurité**, qui améliorera la coordination et la coopération entre les États membres et les institutions, organismes et organes de l'UE;
- **établir un cadre de certification à l'échelle l'UE** qui assurera la fiabilité de milliards de dispositifs («Internet des objets») qui pilotent dorénavant les infrastructures critiques, telles que les réseaux d'énergie et de transport, mais aussi de nouveaux équipements grand public, tels que les voitures connectées.

Une Agence européenne pour la cybersécurité: l'Agence disposerait d'un **mandat permanent** pour aider les États membres à prévenir efficacement les cyberattaques et à y répondre.

En vue d'améliorer la préparation de l'UE en cas d'attaques, elle organiserait chaque année des **exercices de cybersécurité paneuropéens** et assurerait un meilleur partage des connaissances et des informations sur les menaces par la création de **centres de partage et d'analyse de l'information**.

Elle contribuerait aussi à la mise en œuvre de la directive SRI, qui impose des obligations de signalement des incidents graves aux autorités nationales.

L'Agence aiderait en outre à créer et à appliquer le cadre de certification à l'échelle de l'UE proposé par la Commission pour garantir que les produits et les services répondent à toutes les exigences de cybersécurité applicables.

La proposition comprend également les dispositions visant à faciliter la **lutte contre la fraude, la corruption et d'autres activités illégales**, ainsi que des dispositions en matière de dotation en personnel et de budget.

Un cadre de certification de la cybersécurité de l'UE: actuellement, il existe différents systèmes de certification de sécurité pour les produits TIC dans l'UE. L'Agence mettra en place un processus de certification. Le cadre de certification proposé à l'échelle de l'UE crée un **ensemble complet de règles, d'exigences techniques, de normes et de procédures** destiné à convenir à chaque système. Chaque système de certification serait basé sur un accord au niveau de l'UE pour l'évaluation des propriétés de sécurité d'un produit TIC spécifique (par exemple : carte à puce).

La proposition établit les **principaux effets juridiques** des systèmes européens de certification de la cybersécurité, à savoir: i) l'obligation de mettre en œuvre le régime au niveau national et le **caractère volontaire** de la certification; ii) l'effet invalidant des systèmes de certification de la cybersécurité européenne sur les régimes nationaux pour les mêmes produits ou services. Elle définit également la procédure d'adoption des systèmes européens de certification ainsi que les rôles respectifs de la Commission, de l'Agence et du Groupe européen de certification de la cybersécurité.

INCIDENCE BUDGÉTAIRE: le total des crédits, y compris les dépenses administratives, de 2019 à 2022 est estimé à **86,038 millions d'EUR**.